$\mathbb{Z}/p$ metabelian birational p-adic section conjecture for varieties

Florian Pop

Abstract

We generalize the $\mathbb{Z}/p$ *metabelian* birational p-adic section conjecture for curves, as introduced and proved in Pop [P2], to all complete smooth varieties, provided $p > 2$. [The condition $p > 2$ seems to be of technical nature only, and it might be removable.]

1. Introduction

The (birational) [p-adic] section conjecture (SC) originates from GROTHENDIECK [G1], [G1], see rather [GGA], and weaker/conditional forms of the SC are a part of the *local theory* in anabelian geometry, see e.g. FALTINGS [Fa] and SZAMUELY [Sz]. In spite of serious efforts to tackle the SC, only the *full Galois birational p-adic* SC is completely resolved, see KOENIGSMANN [Ko2] for the case of curves, and STIX [St] for higher dimensional varieties. On the other hand, a much stronger form of the birational p-adic SC for curves, to be precise, the $\mathbb{Z}/p$ *metabelian* birational p-adic SC for curves was proved in POP [P2]. The aim of this note is to prove a similarly strong result for the *higher dimensional varieties,* at least in the case $p > 2$.

For reader's sake and to make the presentation self contained (to some extent), we begin by recalling a few notations and well known facts, see e.g. the Introduction in [P2]. First, for an arbitrary (perfect) base field k, and complete smooth geometrically integral k-varieties X, let $K = k(X)$ be the function field of X. Let $\tilde{K}|K$ be some Galois extension, $\tilde{k} \subseteq \tilde{K}$ be the relative algebraic closure of k in $\tilde{K}$, and consider the resulting canonical exact sequence of Galois groups:

$$1 \to \mathrm{Gal}(\tilde{K}|K\tilde{k}) \longrightarrow \mathrm{Gal}(\tilde{K}|K) \xrightarrow{\tilde{p}_K} \mathrm{Gal}(\tilde{k}|k) \to 1\,.$$

Let $\tilde{X} \to X$ be the normalization of X in the field extension $K \hookrightarrow \tilde{K}$. For $x \in X$ and $\tilde{x} \in \tilde{X}$ above x, let $T_x \subseteq Z_x$ be the inertia/decomposition, groups of $\tilde{x}|x$, and $G_x := \mathrm{Aut}\big(\kappa(\tilde{x})|\kappa(x)\big)$ be the residual automorphism group. By decomposition theory, one has a canonical exact sequence

$$(*) \qquad 1 \to T_x \to Z_x \to G_x \to 1\,.$$

Next suppose that x is k-rational, i.e., $\kappa(x) = k$. Since $\tilde{k} \subset \kappa(\tilde{x})$, the projection $Z_x \xrightarrow{\tilde{p}_K} \mathrm{Gal}(\tilde{k}|k)$ gives rise to a canonical surjective homomorphism $G_x \to \mathrm{Gal}(\tilde{k}|k)$, which in general is not injective. And if $\kappa(\tilde{x})|\tilde{k}$ is purely inseparable, then the canonical homomorphism $G_x \to \mathrm{Gal}(\tilde{k}|k)$ is an isomorphism. Hence if the exact sequence $(*)$ splits, then $\tilde{p}_K$ has sections $\tilde{s}_x : \mathrm{Gal}(\tilde{k}|k) \to Z_x \subset \mathrm{Gal}(\tilde{K}|K)$, which we call sections above x; and notice that the conjugacy classes of sections $\tilde{s}_x$ above x build a "bouquet", which is in a canonical bijection with the (non-commutative) continuous cohomology

---

2000 Mathematics Subject Classification Primary 11G, 14G; Secondary 12E30

Keywords: anabelian geometry, absolute Galois groups, p-adically closed fields, rational points, valuations, Hilbert decomposition theory, (birational) section conjecture.

Variant of Apr 8, 2015.

Supported by NSF grant DMS–1101397. Parts of this research were partially performed while visiting the MPIM Bonn in May 2012 and HIM Bonn in spring 2013. I would like to thank these Institutions for the wonderful research environment and the excellent working conditions.

pointed set $\mathrm{H}^1_{\mathrm{cont}}\big(\mathrm{Gal}(\tilde{k}|k), T_x\big)$ defined via the split exact sequence $(*)$.

Parallel to the case of points $x \in X$, one has a similar situation for k-valuations v of K as follows. For any prolongation $\tilde{v}$ of v to $\tilde{K}$, we denote by $T_v \subseteq Z_v$ the inertia/decomposition groups of $\tilde{v}|v$, and by $G_v = Z_v/T_v$ the residual automorphism group. As above, if $\kappa(v) = k$ and $\kappa(\tilde{v})|\tilde{k}$ is purely inseparable, one has: First, the canonical homomorphism $G_v \to \mathrm{Gal}(\tilde{k}|k)$ is an isomorphism. Second, if the exact sequence $1 \to T_v \to Z_v \to G_v \to 1$ splits, then $\tilde{p}_K : \mathrm{Gal}(\tilde{K}|K) \to \mathrm{Gal}(\tilde{k}|k)$ has a section $\tilde{s}_v : \mathrm{Gal}(\tilde{k}|k) \to Z_v \subseteq \mathrm{Gal}(\tilde{K}|K)$, which we call a section above v. And the conjugacy classes of sections $\tilde{s}_v$ above v build a "bouquet" which is in a canonical bijection with the (non-commutative) continuous cohomology pointed set $\mathrm{H}^1_{\mathrm{cont}}\big(\mathrm{Gal}(\tilde{k}|k), T_v\big)$ defined via the canonical split exact sequence above.

Finally, if $\tilde{K}|K$ contains a separable closure $K^{\mathrm{s}}|K$ of K, hence $\tilde{k} \supseteq k^{\mathrm{s}}$ too, then $\kappa(s)^{\mathrm{s}} \subseteq \kappa(\tilde{x}), \kappa(\tilde{v})$ and G_x and G_v are the absolute Galois groups of $\kappa(x)$, respectively $\kappa(v)$. Further, in this situation, the canonical exact sequence $1 \to T_v \to Z_v \to G_v \to 1$ is split, see e.g., [KPR]. Thus if $\kappa(v) = k$, sections above v exist. In particular, if $x \in X(k)$ is a k-rational point, then choosing v such that $\kappa(x) = \kappa(v)$, it follows that sections above x exist as well, because every section above v is a section above x as well. We mention though that in general the bouquet of sections above x is much richer than the one of sections above v. Indeed, by general decomposition theory one has $T_v \subset T_x$, and the canonical map $\mathrm{H}^1_{\mathrm{cont}}\big(\mathrm{Gal}(\tilde{k}|k), T_v\big) \to \mathrm{H}^1_{\mathrm{cont}}\big(\mathrm{Gal}(\tilde{k}|k), T_x\big)$ is a strict inclusion in general.

• Next let p be a fixed prime number. We denote by $K'|K$ the (maximal) $\mathbb{Z}/p$ elementary abelian extension of K, and by K'' the maximal $\mathbb{Z}/p$ elementary abelian extension of K' (in some fixed algebraic closure of K). Then $K''|K$ is a Galois extension, which we call the $\mathbb{Z}/p$ metabelian extension of K, and its Galois group $\mathrm{Gal}(K''|K)$ is called the metabelian Galois group of K. Note that $k' := \overline{k} \cap K'$, and $k'' := \overline{k} \cap K''$ are the $\mathbb{Z}/p$ elementary abelian extension, respectively the $\mathbb{Z}/p$ metabelian extension, of k. Finally, consider the canonical surjective projections:

$$pr'_K : \mathrm{Gal}(K'|K) \to \mathrm{Gal}(k'|k), \quad pr''_K : \mathrm{Gal}(K''|K) \to \mathrm{Gal}(k''|k).$$

We will say that a group theoretical (continuous) section $s' : \mathrm{Gal}(k'|k) \to \mathrm{Gal}(K'|K)$ of pr'_K is liftable, if there exists a section $s'' : \mathrm{Gal}(k''|k) \to \mathrm{Gal}(K''|K)$ of pr''_K which lifts s' to $\mathrm{Gal}(k''|k)$.

Note that if $p \neq$ char, and the p^{th} roots of unity μ_p are contained in k, hence in K, then by Kummer Theory we have: $K' = K[\sqrt[p]{K}\,]$, and $K'' = K'[\sqrt[p]{K'}\,]$, and similarly for k.

Theorem A. *In the above notations, let $k|\mathbb{Q}_p$ be finite with $\mu_p \subset k$. Then the following hold:*

1) *Every k-rational point $x \in X$ gives rise to a bouquet of conjugacy classes of liftable sections $s'_x : \mathrm{Gal}(k'|k) \to \mathrm{Gal}(K'|K)$ above x, which is in bijection with $\mathrm{H}^1\big(\mathrm{Gal}(k'|k), T_x\big)$.*
2) *Let $p > 2$, and $s' : \mathrm{Gal}(k'|k) \to \mathrm{Gal}(K'|K)$ be a liftable section. Then there exists a unique k-rational point $x \in X$ such that s' equals one of the sections s'_x as defined above.*

Actually one can reformulate the question addressed by Theorem A in terms of p-adic valuations, and get the following stronger result, see Section 2, C), for notations, definitions, and a few facts on (formally) p-adic valuations v, e.g., the p-adic rank d_v of v, and p-adically closed fields, respectively Ax–Kochen [A–K] and Prestel–Roquette [P–R], for proofs:

Theorem B. *Let k be a p-adically closed field with p-adic valuation v of p-adic rank d_v, and suppose that $\mu_p \subset k$. Let $K|k$ be an arbitrary field extension. Then the following hold:*

1) *Let w be a p-adic valuation of K of p-adic rank $d_w = d_v$. Then w prolongs v to K, and gives rise to a bouquet of conjugacy classes of liftable sections $s'_w : \mathrm{Gal}(k'|k) \to \mathrm{Gal}(K'|K)$ above w.*

2) *Let $p > 2$, and $s' : \mathrm{Gal}(k'|k) \to \mathrm{Gal}(K'|K)$ be a liftable section. Then there exists a unique p-adic valuation w of K of p-adic rank $d_w = d_v$ such that $s' = s'_w$ for some s'_w as above.*

Remark/Definition. As mentioned in Pop [P2], the condition $\mu_p \subset k$ is a necessary condition in the above theorems. Nevertheless, as mentioned in loc.cit., if μ_p is not contained in the base field, assertions similar to Theorems A and B above hold in the following form: Let $l|\mathbb{Q}_p$ be some finite extension, $Y \to l$ a complete geometrically integral smooth variety with function field $L = \kappa(Y)$. Let $k|l$ be a finite Galois extension with $\mu_p \subset k$. Setting $K := Lk$, consider the field extensions $K'|K \hookrightarrow K''|K$ and $k'|k \hookrightarrow k''|k$ as above. Then $k' = K' \cap \bar{l}$ and $k'' = K'' \cap \bar{l}$, and $K'|L$ and $K''|L$, as well as $k'|l$ and $k''|l$ are Galois extensions too, and one gets surjective canonical projections

$$pr'_L : \mathrm{Gal}(K'|L) \to \mathrm{Gal}(k'|l), \quad pr''_L : \mathrm{Gal}(K''|L) \to \mathrm{Gal}(k''|l).$$

In these notations and context we will say that a section $s'_L : \mathrm{Gal}(k'|l) \to \mathrm{Gal}(K'|L)$ of pr'_L is liftable, if there exists a section $s''_L : \mathrm{Gal}(k''|l) \to \mathrm{Gal}(K''|L)$ of pr''_L which lifts s'_L.

This being said, one has the following extensions of Theorem A and Theorem B:

Theorem A^0. *In the above notations and hypothesis, the following hold:*

1) *Every l-rational point $y \in Y$ gives rise to a bouquet of conjugacy classes of liftable sections $s'_y : \mathrm{Gal}(k'|l) \to \mathrm{Gal}(K'|L)$ above y, which is in bijection with $\mathrm{H}^1\big(\mathrm{Gal}(k'|l), T_y\big)$.*
2) *Let $p > 2$ and $s'_L : \mathrm{Gal}(k'|l) \to \mathrm{Gal}(K'|L)$ be a liftable section. Then there exists a unique l-rational point $y \in Y$ such that s'_L equals one of the sections s'_y as defined above.*

Theorem B^0. *Let l be a p-adically closed field with p-adic valuation v, and let $L|l$ be an arbitrary field extension. Then in the above notations the following hold:*

1) *Let w be a p-adic valuation of L with $d_w = d_v$. Then w prolongs v to L, and gives rise to a bouquet of conjugacy classes of liftable sections $s'_w : \mathrm{Gal}(k'|l) \to \mathrm{Gal}(K'|L)$ above w.*
2) *Let $p > 2$ and $s'_L : \mathrm{Gal}(k'|l) \to \mathrm{Gal}(K'|L)$ be a liftable section. Then there exists a unique p-adic valuation w of L such that $d_w = d_v$, and s'_L equals one of the sections s'_w as above.*

Remark. As mentioned in Pop [P2], the $\mathbb{Z}/p$ metabelian form of the birational p-adic SC for curves implies the corresponding full Galois SC, which was proved in Koenigsmann [Ko2]. The same hold correspondingly for higher dimensional varieties, provided $p > 2$, thus implying Stix [St] result in this case. Since the proof of the implication under discussion in the case of general varieties is word-by-word the same as that from [P2] loc.cit., we will not reproduce it here.

An interesting application of the results and techniques developed here is the following fact concerning the p-adic Section Conjecture for varieties: Let $k|\mathbb{Q}_p$ be a finite extension, and X a complete smooth k-variety. Then there exists a finite effectively computable family of finite geometrically $\mathbb{Z}/p$ elementary abelian (ramified) covers $\varphi_i : X_i \to X$, $i \in I$, satisfying:

i) $\cup_i \varphi_i\big(X_i(k)\big) = X(k)$, i.e., every $x \in X(k)$ "survives" in at least one of the covers $X_i \to X$.
ii) A section $s : G_k \to \pi_1(X, *)$ can be lifted to a section $s_i : G_k \to \pi_1(X_i, *)$ for some $i \in I$ if and only if s arises from a k-rational point $x \in X(k)$ in the way described above.

The main technical tools for the proof of the above theorems are:

- The techniques developed in Pop [P2] (which refine facts/methods initiated in [P1]).
- The theory of rigid elements, as developed by several people: Ware [Wa], Arason–Jacob–Ware [AJW], Koenigsmann [Ko1], Efrat [Ef], etc. But see rather Topaz [To].

As a final remark, we notice that the condition $p > 2$ in the results above originates from the weaker results about recovering valuations from rigid elements in the case $p = 2$. This technical condition might be removable, but some new ideas/techniques might be necessary to do so, see the comment at the beginning of the proof of assertion 2) of Theorem B in section 3.

2. Reviewing a few known facts

For reader's sake, in this section we review a few known facts about valuation theory, decomposition theory, and (formally) p-adic fields, but do not reproduce proofs.

A) *Generalities about valuations and their Hilbert decomposition theory*

For an arbitrary field K and an arbitrary valuation v of K, we denote usually by $\mathcal{O}_v, \mathfrak{m}_v$ the valuation ring/ideal of v, by $vK = K^\times/\mathcal{O}^\times$ the value group of v, and by $Kv =: \mathcal{O}_v/\mathfrak{m}_v := \kappa(v)$ the residue field of v. Further, $U_v^1 := 1 + \mathfrak{m}_v \subset U_v$ denote the groups of principal v-units, respectively v-units. One has the following canonical exact sequences:

$$1 \to \mathfrak{m}_v \to \mathcal{O}_v \to Kv \to 0 \quad \text{and} \quad 1 \to U_v^1 \to {\mathcal{O}^\times}_v \to (Kv)^\times \to 1.$$

The set of ideals of $\mathcal{O}_v$ is totally ordered with respect to inclusion. The subrings $\mathcal{O}_1 \subseteq K$ with $\mathcal{O}_v \subseteq \mathcal{O}_1$ are precisely the localizations $\mathcal{O}_1 := (\mathcal{O}_v)_{\mathfrak{m}_1}$ with $\mathfrak{m}_1 \in \mathrm{Spec}(\mathcal{O}_v)$, and moreover, $\mathfrak{m}_1 \subset \mathcal{O}_v$, and $(\mathcal{O}_v)_{\mathfrak{m}_1}$ is a valuation ring with valuation ideal $\mathfrak{m}_1$. Further, if v_1 is the corresponding valuation of K, then $\mathcal{O}_0 := \mathcal{O}_v/\mathfrak{m}_1$ is a valuation ring of Kv_1 with valuation ideal $\mathfrak{m}_0 := \mathfrak{m}_v/\mathfrak{m}_1$, say of a valuation v_0 of Kv_1. We say that v_1 is a coarsening of v, and denote $v_1 \leqslant v$ and $v_0 := v/v_1$.

Conversely, if v_1 is a valuation of K and v_0 is a valuation on the residue field Kv_1, then the preimage of the valuation ring $\mathcal{O}_{v_0} \subseteq Kv_1$ under $\mathcal{O}_{v_1} \to Kv_1$ is a valuation ring $\mathcal{O} \subseteq \mathcal{O}_{v_1}$ having as valuation ideal the preimage $\mathfrak{m} \subset \mathcal{O}$ of $\mathfrak{m}_{v_0}$. Hence if v is the valuation defined by $\mathcal{O}$ on K, then $Kv = (Kv_1)v_0$ and one has a canonical exact sequence of totally ordered groups:

$$0 \to v_0(Kv_1) \to vK \to v_1K \to 0.$$

The relation between coarsening and decomposition theory is as follows. Let $\tilde{K}|K$ be a Galois extension, and $\tilde{v}|v$ be a prolongation of v to $\tilde{K}$. Then the coarsenings $\tilde{v}_1$ of $\tilde{v}$ are in a canonical bijection with the coarsenings v_1 of v via $\mathcal{O}_{\tilde{v}_1} \mapsto \mathcal{O}_{v_1} := \mathcal{O}_{\tilde{v}_1} \cap K$, thus $\mathcal{O}_{\tilde{v}_1} = \mathcal{O}_{\tilde{v}} \cdot \mathcal{O}_{v_1}$. Let $\tilde{v}_1|v_1$ be given coarsenings of $\tilde{v}|v$ and $\tilde{K}\tilde{v}_1|Kv_1$ is the corresponding residue field extension. Then $\tilde{v}_0 := \tilde{v}/\tilde{v}_1$ is canonically a prolongation of $v_0 := v/v_1$.

Fact 1. *Let $T_{\tilde{v}} \subseteq Z_{\tilde{v}}$ and $T_{\tilde{v}_1} \subseteq Z_{\tilde{v}_1}$ be the corresponding inertia/decomposition groups, and set $G_{\tilde{v}_1} = \mathrm{Aut}(\tilde{K}\tilde{v}_1|Kv_1)$. Then one has a canonical exact sequence $1 \to T_{\tilde{v}_1} \to Z_{\tilde{v}_1} \to G_{\tilde{v}_1} \to 1$, and the inertia/decomposition groups satisfy:*

- *a) $Z_{\tilde{v}} \subseteq Z_{\tilde{v}_1}$ and $T_{\tilde{v}} \supseteq T_{\tilde{v}_1}$. Further, $T_{\tilde{v}_1}$ is a normal subgroup of $Z_{\tilde{v}}$.*
- *b) Via $1 \to T_{\tilde{v}_1} \to Z_{\tilde{v}_1} \to G_{\tilde{v}_1} = Z_{\tilde{v}_1}/T_{\tilde{v}_1} \to 1$, one has that $T_{\tilde{v}_0} = T_{\tilde{v}}/T_{\tilde{v}_1}$ and $Z_{\tilde{v}_0} = Z_{\tilde{v}}/T_{\tilde{v}_1}$.*

B) *Hilbert decomposition in elementary abelian extensions*

Let K be a field of characteristic prime to p containing μ_n, where $n = p^e$ is a power of the prime number p, and let $\tilde{K} = K[\sqrt[n]{K}]$ be the maximal $\mathbb{Z}/n$ elementary abelian extension of K. Let v be a valuation of K, and $\tilde{v}$ some prolongation of v to $\tilde{K}$, and $V_{\tilde{v}} \subseteq T_{\tilde{v}} \subseteq Z_{\tilde{v}}$ be the ramification, the inertia, and the decomposition, groups of $\tilde{v}|v$, respectively. We remark that because $\mathrm{Gal}(\tilde{K}|K)$ is commutative, the groups $V_{\tilde{v}}$, $T_{\tilde{v}}$, and $Z_{\tilde{v}}$ depend on v only. Therefore we will simply denote them by V_v, T_v, and Z_v. Finally, we denote by $K^Z \subseteq K^T \subseteq K^V$ the corresponding fixed fields in $\tilde{K}$. One has the following, see e.g. Pop [P2], Section 2 (where the case $n = p$ is dealt with; but the proof is absolutely similar for general $n = p^e$ and we will not reproduce the details here again):

Fact 2. *In the above notations, the following hold:*

1) *Let* $U^v := 1+p^{2e}\mathfrak{m}_v$. *Then* K^Z *contains* $\sqrt[n]{U^v}$, *and* $K^Z = K[\sqrt[n]{1+\mathfrak{m}_v}\,]$, *provided* $\mathrm{char}(Kv) \neq p$. *In particular, if* w_1 *and* w_2 *are independent valuations of* K, *then* $Z_{w_1} \cap Z_{w_2} = 1$.
2) *If* $p \neq \mathrm{char}(Kv)$, *then* $V_v = 1$ *and* $\tilde{K}\tilde{v} = \widetilde{Kv}$, *hence* $G_v := Z_v/T_v = \mathrm{Gal}(\widetilde{Kv}|Kv)$ *in this case. And if* $p = \mathrm{char}(Kv)$, *then* $V_v = T_v$, *and the residue field* $\tilde{K}\tilde{v}$ *contains* $(Kv)^{\frac{1}{n}}$ *and a maximal* $\mathbb{Z}/n$ *elementary abelian extension of* Kv.
3) *Let* $L := K^{\mathrm{h}}_v$ *be the Henselization of* K *with respect to* v. *Then* $\tilde{L} = L\tilde{K}$ *is a maximal* $\mathbb{Z}/n$ *elementary extension of* L. *Therefore we have* $\mathrm{Gal}(\tilde{L}|L) \cong Z_{\tilde{v}}$ *canonically.*

C) *Formally* p*-adic fields and* p*-adic valuations*

We recall a few basic facts about p-adic valuations and (formally) p-adically closed fields, see Ax–Kochen [A–K] and Prestel–Roquette [P–R] for more details.

1) A valuation v of a field k is called (formally) p-adic, if its residue field kv is a finite field, say $\mathbb{F}_q$ with $q = p^{f_v}$ elements, and the value group vk has a minimal positive element 1_v such that $v(p) = e_v \cdot 1_v$ for some natural number $e_v > 0$. The number $d_v := e_v f_v$ is called the p-adic rank (or degree) of the p-adic valuation v. Note that a field k carrying a p-adic valuation v must necessarily have $\mathrm{char}(k) = 0$, as $v(p) \neq \infty$, and $\mathrm{char}(kv) = p$.
2) Let v be a p-adic valuation of k with valuation ring $\mathcal{O}_v$. Then $\mathcal{O}_1 := \mathcal{O}_v[1/p]$ is the valuation ring of the unique maximal proper coarsening v_1 of v, which is called the canonical coarsening of v. Note that setting $k_0 := kv_1$, and $v_0 := v/v_1$ the corresponding valuation on k_0 we have: v_0 is a p-adic valuation of k_0 with $e_{v_0} = e_v$ and $f_{v_0} = f_v$, hence $d_{v_0} = d_v$, and moreover, v_0 is a discrete valuation of k_0. In particular, the following hold:
   a) v has rank one iff v_1 is the trivial valuation iff $v = v_0$.
   b) Giving a p-adic valuation v of a field k of p-adic rank $d_v = e_v f_v$ is equivalent to giving a place $\mathfrak{p}$ of k with values in a finite extension $\boldsymbol{k}_0$ of $\mathbb{Q}_p$ such that the residues field $k_0 := k\mathfrak{p}$ of $\mathfrak{p}$ is dense in $\boldsymbol{k}_0$, and $\boldsymbol{k}_0|\mathbb{Q}_p$ has ramification index e_v and residual degree f_v.
   c) If $v_i < v$ is a strict coarsening of v, then $v_i \leqslant v_1$, and the quotient valuation v/v_i on the residue field kv_i is a p-adic valuation with $e_{v/v_i} = e_v$ and $f_{v/v_i} = f_v$, thus $d_{v/v_i} = d_v$. (Actually, $\kappa(v_i/v_1) \cong kv_1$ and $\kappa(v_i/v) \cong kv$ canonically.)
3) Let v be a p-adic valuation of k, and $l|k$ a finite field extension, and $w|v$ denote the prolongations of v to l. Then the following hold:
   a) All prolongations $w|v$ are p-adic valuations. Further, the *fundamental equality* holds for the finite extension $l|k$, i.e, $[l:k] = \sum_{w|v} e(w|v)f(w|v)$, where $e(w|v)$ and $f(w|v)$ are the ramification index, respectively the residual degree of $w|v$.
   b) For each $w|v$, let w_1 be the canonical coarsening of w, and $w_0 = w/w_1$ be the canonical quotient on the residue field lw_1. Then by general decomposition theory of valuations one has: $e(w|v) = e(w_1|v_1)e(w_0|v_0)$ and $f(w|v) = f(w_0|v_0)$. Further, $e_w = e(w_0|v_0)e_v$, and $f_w = f(w|v)f_v$, thus $d_w = e(w_0|v_0)f(w|v)\,d_v$.
   c) In particular, if $l|k$ is Galois, and w^Z is the restriction of w to the decomposition field l^Z of w, then $e(w|w^Z) = e(w|v)$ and $f(w|w^Z) = f(w|v)$, thus w^Z is a p-adic valuation having p-adic rank equal to the one of v. Further, the same is true for infinite Galois extensions $l|k$.
4) A field k is called (formally) p-adically closed, if k carries a p-adic valuation v such that for every finite extension $\tilde{k}|k$ one has: If v has a prolongation $\tilde{v}$ to $\tilde{k}$ with $d_{\tilde{v}} = d_v$, then $\tilde{k} = k$. One has the following characterization of the p-adically closed fields: For a field k endowed with a p-adic valuation v, and its canonical coarsening v_1, the following are equivalent:

i) k is p-adically closed with respect to v.

ii) v is Henselian, and $v_1 k$ is divisible (maybe trivial).

iii) v_1 is Henselian, $v_1 k$ is divisible (maybe trivial), and the residue field $k_0 := kv_1$ is relatively algebraically closed in its $v_0 = v/v_1$ completion $\boldsymbol{k}_0$ (which itself is a finite extension of $\mathbb{Q}_p$).

Further, the p-adic valuation of a p-adically closed field is definable and unique.

5) Finally, for every field k endowed with a p-adic valuation v, there exist p-adic closures $\widehat{k}, \widehat{v}$ such that $d_{\widehat{v}} = d_v$. Moreover, the space of the k-isomorphy classes of p-adic closures of k, v has a concrete description as follows: Let v_1 be the canonical coarsening of v, and $\boldsymbol{k}_0|\mathbb{Q}_p$ the completion of the residue field of $k_0 = kv_1$ with respect to the discrete valuation $v_0 = v/v_1$. Recalling the canonical exact sequence $1 \to I_{v_1} \longrightarrow D_v \xrightarrow{pr} G_{\boldsymbol{k}_0} \to 1$, one has that the space of the isomorphy classes of p-adic closures of k, v is in bijection with the space of conjugacy classes of sections of pr, thus with $\mathrm{H}^1_{\mathrm{cont}}(G_{\boldsymbol{k}_0}, I_{v_1})$.

6) In the above notations, the following hold:

a) Let k, v be a p-adically closed field. Then $k_0 = kv_1$ is p-adically closed (with respect to v_0), and k^{abs} is actually the relative algebraic closure of $\mathbb{Q}$ in k_0. Further, $\overline{k} = k\overline{\mathbb{Q}}$.

b) The elementary equivalence class of a p-adically closed field k is determined by both: The *absolute subfield* $k^{\mathrm{abs}} := k \cap \overline{\mathbb{Q}} = k_0 \cap \overline{\mathbb{Q}}$ of k, and the *completion* $\boldsymbol{k}_0$ of $k_0 = kv_1$ with respect to v_0 (which equals the completion of k^{abs} with respect to v_0 as well).

c) If N is p-adically closed with respect to the p-adic valuation w, and $k \subseteq N$ is a subfield which is relatively closed in N, then k is p-adically closed with respect to $v := w|_k$, and v and w have equal p-adic ranks, and N and k are elementary equivalent.

d) If $N|k$ is an extension of p-adically closed fields of the same rank, the following hold:

- $\tilde{k}|k \mapsto N\tilde{k}$ defines a bijection between the algebraic extensions $\tilde{k}|k$ of k and those of N.
- The canonical projection $G_N \to G_k$ is an isomorphism.

e) In particular, if $L|l$ is an extension of p-adically closed fields of the same rank, in the notations from the Introduction, the following canonical projections are isomorphisms:

$$(\dagger) \qquad pr'_L : \mathrm{Gal}(K'|L) \to \mathrm{Gal}(k'|l), \quad pr''_L : \mathrm{Gal}(K''|L) \to \mathrm{Gal}(k''|l).$$

D) *Valuations and rigid elements*

We recall the result ARASON–ELMAN–JAKOB [AEJ], Theorem 2.16, see also KOENIGSMAN [Ko1], WARE [Wa], EFRAT [Ef], and rather TOPAZ [To] for much more about this. The point here is that one can recover valuations of an arbitrary field K from particular subgroups $T \subset K^\times$ as follows: Let $T \subset K^\times$ be a subgroup with $-1 \in T$. We say that $x \in K^\times \backslash T$ is T-rigid, if $1 + x \in T \cup xT$; and by abuse of language, we say that that K is T-rigid, if all $x \in K^\times \backslash T$ are T-rigid.

THEOREM 3 (Arason-Elman-Jacob). *In the above notations, let $T \subset K^\times$ be a subgroup with $-1 \in T$ such that K is T-rigid. Then there exist a valuation v of K whose valuation ideal $\mathfrak{m}_v$ satisfies $1 + \mathfrak{m}_v \subseteq T$, and whose valuation ring $\mathcal{O}_v$ has the property that $\left|\mathcal{O}_v^\times/(T \cap \mathcal{O}_v^\times)\right| \leqslant 2$.*

3. Proof of Theorem B

To 1): Let $\widehat{K}, \widehat{w}$ be a p-adic closure of K, w. Then $\widehat{w}$ prolongs w and has p-adic rank $d_{\widehat{w}} = d_w$, thus equal to d_v by the fact that $d_w = d_v$. Therefore, since k is p-adically closed, k must be relatively algebraically closed in $\widehat{K}$. Conclude by applying relation ($\dagger$) from Section 2, C), 6), e), with $l := k$ and $L := \widehat{K}$, and taking into account that the isomorphisms $\mathrm{Gal}(\widehat{K}''|\widehat{K}) \to \mathrm{Gal}(k''|k)$ factors through $\mathrm{Gal}(K''|K) \to \mathrm{Gal}(k''|k)$, thus gives rise to a liftable section of $\mathrm{Gal}(K'|K) \to \mathrm{Gal}(k'|k)$.

To 2): The proof of assertion 2) is divided in three main steps, whereas the hypothesis $p > 2$ is used only in Step 2). This might be relevant when trying to address the case $p = 2$.

Step 1. By Kummer theory, $pr'_K : \mathrm{Gal}(K'|K) \to \mathrm{Gal}(k'|k)$ is Pontrjagin dual to the canonical embedding $k^\times/p \to K^\times/p$. Second, given a liftable section $s' : \mathrm{Gal}(k'|k) \to \mathrm{Gal}(K'|K)$ of pr'_K, it follows by Kummer theory that the Pontrjagin dual of $s' : \mathrm{Gal}(k'|k) \to \mathrm{Gal}(K'|K)$ is a surjective projection $K^\times/p \to k^\times/p$, whose kernel $\Sigma/p \subset K^\times/p$ is a complement of $k^\times/p \subset K^\times/p$. That means, s' gives rise canonically to a presentation of $K^\times/p$ as a direct sum

$$(\dagger) \qquad K^\times/p = \Sigma/p \cdot k^\times/p\,.$$

For every k-subfield $K_\alpha \subset K$ which is relatively algebraically closed in K, one has a commutative diagram of surjective projections

$$\begin{array}{ccccc}
\mathrm{Gal}(K''|K) & \longrightarrow & \mathrm{Gal}(K''_\alpha|K_\alpha) & \longrightarrow & \mathrm{Gal}(k''|k) \\
\downarrow & & \downarrow & & \downarrow \\
\mathrm{Gal}(K'|K) & \longrightarrow & \mathrm{Gal}(K'_\alpha|K_\alpha) & \longrightarrow & \mathrm{Gal}(k'|k)
\end{array}$$

and s' gives rise canonically to a liftable section s'_α of $pr'_\alpha : \mathrm{Gal}(K'_\alpha|K_\alpha) \to \mathrm{Gal}(k'|k)$, etc. In particular, one has corresponding canonical presentations as direct sums

$$(\dagger)_\alpha \qquad K^\times_\alpha/p = \Sigma_\alpha/p \cdot k^\times/p$$

defined by the liftable sections $s'_\alpha : \mathrm{Gal}(k'|k) \to \mathrm{Gal}(K'_\alpha|K_\alpha)$ induced by $s' : \mathrm{Gal}(k'|k) \to \mathrm{Gal}(K'|K)$.

Claim. *In the above notions one has: $\Sigma_\alpha/p = \Sigma/p \cap K^\times_\alpha/p$, thus Σ/p determines Σ_α/p.*

Indeed, let $D_\alpha := \mathrm{im}(s'_\alpha) \subset \mathrm{Gal}(K'_\alpha|K_\alpha)$. Then by the definition of s'_α, it follows that D_α is the image of $D = \mathrm{im}(s')$ under the canonical projection $\mathrm{Gal}(K'|K) \to \mathrm{Gal}(K'_\alpha|K_\alpha)$. In other words, by Pontrjagin duality, the projection $K^\times_\alpha/p \to k^\times/p$ factors through the inclusion $K^\times_\alpha/p \hookrightarrow K^\times/p$. Hence Σ_α/p is mapped into Σ/p under $K^\times_\alpha/p \hookrightarrow K^\times/p$, which proves th Claim.

Now let $T/p := \Sigma/p \cdot \mathcal{O}^\times_v/p$ and $T \subset K^\times$ be the corresponding subgroup (thus containing the p^{th} powers in $K^\times$). Then for every k-subfield $K_\alpha \subset K$ which is relatively algebraically closed in K, by the remarks above one has that $T_\alpha := T \cap K^\times_\alpha \subset K^\times_\alpha$ satisfies $T_\alpha/p = \Sigma_\alpha/p \cdot \mathcal{O}^\times_v/p$.

Finally, let $(K_\alpha)_\alpha$ be the family of all the k-subfields $K_\alpha \subset K$ which are relatively algebraically closed in K and satisfy $\mathrm{tr.deg}(K_\alpha|k) = 1$. Then by Theorem B of Pop [P2], for every subfield K_α, there exits a unique p-adic valuation w_α of K_α prolonging the p-adic valuation v of k to K_α and having the same p-adic rank as v. Our final aim is to show that there exists a (unique) p-adic valuation w of K such that w_α is the restriction of w to K_α for each K_α.

Lemma 4. *In the above notations, K_α is T_α rigid. Further, $T = \cup_\alpha T_\alpha$, and K is T-rigid.*

Proof. We first show that $\mathcal{O}_{w_\alpha} \subset T_\alpha$. Indeed, let v be the p-adic valuation of k, and further consider: First, the canonical coarsening v_1 of v, and the canonical p-adic valuation $v_0 := v/v_1$ on the residue field $k_0 := kv_1$ of v_1. Second, for the p-adic valuation w_α of K_α, let $w_{\alpha 1}$ and $w_{\alpha 0} := w_\alpha/w_{\alpha 1}$, and $K_{\alpha 0}$ be correspondingly defined. Notice that $w_\alpha|_k = v$ implies that $w_{\alpha 1}|_k = v_1$ and $w_{\alpha 0}|_{k_0} = v_0$. The following hold:

a) First, by Fact 2, it follows that $\sqrt[p]{1 + p^2\mathfrak{m}_{w_\alpha}}$ is contained in the decomposition field of w_α over K, which is actually the fixed field of Z_{w_α} in K'_α. Second, the fixed field of $\mathrm{im}(s')$ in K'_α is, by the mere definitions, generated as a field extension of K by $\sqrt[p]{\Sigma_\alpha}$. Thus since $\mathrm{im}(s') \subset Z_{w_\alpha}$, it follows by Kummer theory that $1 + p^2\mathfrak{m}_{w_\alpha} \subset \Sigma_\alpha$.

b) Since, by the mere definition, one has $\mathfrak{m}_{w_{\alpha 1}} \subset \mathfrak{m}_{w_\alpha}$ and p is invertible in $\mathcal{O}_{w_{\alpha 1}}$, it follows that $1 + \mathfrak{m}_{w_{\alpha 1}} \subset 1 + p^2\mathfrak{m}_{w_\alpha}$. Thus finally, $1 + \mathfrak{m}_{w_{\alpha 1}} \subset \Sigma_\alpha$ as well.

c) Since w_α and v have the same p-adic rank, it follows by the discussion in section 2, C, 5), that $w_{\alpha 0}$ and v_0 are discrete p-adic valuations of the same p-adic rank, hence k_0 is dense in $K_{\alpha 0}$. Therefore, since $w_{\alpha 0}|v_0$ are discrete valuations, and k_0 is dense in $K_{\alpha 0}$ under $k_0 \hookrightarrow K_{\alpha 0}$, one has that $\mathcal{O}^\times_{w_{\alpha 0}} = \mathcal{O}^\times_{v_0} \cdot (1 + p^2\mathfrak{m}_{w_{\alpha 0}})$ and $K^\times_{\alpha 0} = k^\times_0 \cdot (1 + p^2\mathfrak{m}_{w_{\alpha 0}})$ as well.

d) Since $K^\times_{\alpha 0} = \mathcal{O}^\times_{w_{\alpha 1}}/(1 + \mathfrak{m}_{w_{\alpha 1}})$, $k^\times_0 = \mathcal{O}^\times_{v_1}/(1 + \mathfrak{m}_{v_1})$, and $1 + p^2\mathfrak{m}_{w_{\alpha 0}} = (1 + p^2\mathfrak{m}_{w_\alpha})/(1 + \mathfrak{m}_{w_{\alpha 1}})$, from the equality $K^\times_{\alpha 0} = k^\times_0 \cdot (1 + p^2\mathfrak{m}_{w_{\alpha 0}})$ above, it follows that $\mathcal{O}^\times_{w_{\alpha 1}} = \mathcal{O}^\times_{v_1} \cdot (1 + p^2\mathfrak{m}_{w_\alpha})$.

e) Similarly, $\mathcal{O}^\times_{w_{\alpha 0}} = \mathcal{O}^\times_{w_\alpha}/(1+\mathfrak{m}_{w_{\alpha 1}})$ and $\mathcal{O}^\times_{w_{\alpha 0}} = \mathcal{O}^\times_{v_0}\cdot(1+p^2\mathfrak{m}_{w_{\alpha 0}})$, imply $\mathcal{O}^\times_{w_\alpha} = \mathcal{O}^\times{}_v\cdot(1+p^2\mathfrak{m}_{w_\alpha})$.

Hence since $\mathcal{O}^\times_v, 1 + p^2\mathfrak{m}_{w_\alpha} \subset T_\alpha$, one finally has $\mathcal{O}^\times_{w_\alpha} = \mathcal{O}^\times{}_v \cdot (1 + p^2\mathfrak{m}_{w_\alpha}) \subset T_\alpha$, as claimed.

We next show that K_α is T_α-rigid. To do so, we first notice that by the discussion above, for any fixed element $\pi \in \mathcal{O}_v$ of minimal positive value $1_v \in vk$, the following holds: Let $x \in \mathcal{O}^\times_{w_{\alpha 1}}$ be an arbitrary $w_{\alpha 1}$-unit. Then there exist $m \in \mathbb{Z}$, $\epsilon \in \mathcal{O}^\times_v$, $x_1 \in 1 + p^2\mathfrak{m}_{w_\alpha}$ such that

$$(\sharp) \qquad x = \pi^m \epsilon\, x_1.$$

Now let $x \in K^\times_\alpha \backslash T_\alpha$ be given. Then one has the following possibilities:

1) $w_{\alpha 1}(x) > 0$. Then $1+x$ is a principal $w_{\alpha 1}$-unit, and therefore, $1+x \in \Sigma_\alpha$ by assertion b) above. Since $\Sigma_\alpha \subset T_\alpha$, we conclude that $1 + x \in T_\alpha$.

2) $w_{\alpha 1}(x) < 0$. Then $1 + x = x(1 + x^{-1})$. Since $w_{\alpha 1}(x^{-1}) > 0$, by the discussion above, it follows that $1 + x^{-1} \in T_\alpha$. Therefore, one finally has that $1 + x \in xT_\alpha$.

3) $w_{\alpha 1}(x) = 0$, or equivalently, $x \in \mathcal{O}^\times_{w_{\alpha 1}}$. Let $x = \pi^m \epsilon\, x_1$ be as given at ($\sharp$) above. One has:

   α) If $m > 0$, then $x \in \pi^m \cdot \mathcal{O}^\times_{w_\alpha}$, thus $1 + x \in \mathcal{O}^\times_{w_\alpha}$ as well. Hence by the relation ($\sharp$) above, $1 + x = \eta_1 \cdot \eta_0$ for some $\eta_1 \in 1 + p^2\mathfrak{m}_{w_\alpha} \subset \Sigma_\alpha$, $\eta_0 \in \mathcal{O}^\times_v$. Thus finally, $1 + x \in T_\alpha$.

   β) If $m < 0$, then $1 + x = x(1 + x^{-1})$, and x^{-1} has value $-m > 0$. But then, by the first case above, $1 + x^{-1} \in T_\alpha$. Hence $1 + x = x(1 + x^{-1}) \in xT_\alpha$, thus $1 + x \in x\,T_\alpha$.

   γ) If $m = 0$, then $x \in \mathcal{O}^\times_{w_\alpha} \subset T_\alpha$, thus $x \notin K^\times_\alpha \backslash T_\alpha$.

For the T-rigidity of K, let $x \in K\backslash T$ be given. If $x \in k$, then $x \in k\backslash\mathcal{O}^\times_v$ (by the definition of T). An easy case by case analysis, namely $v(x) > 0$ or $v(x) < 0$, shows that $1+x \in \mathcal{O}^\times_v \cup x\,\mathcal{O}^\times_v$, etc. Finally, if $x \notin k$, then letting $K_\alpha \subset K$ be the relative algebraic closure of $k(x)$ in K, one has: Since $x \in K\backslash T$, one must have $x \in K_\alpha\backslash T_\alpha$. Thus by the discussion above, it follows that $1 + x \in T_\alpha \cup x\,T_\alpha$, and therefore, $1 + x \in T \cup x\,T$, etc.

This concludes the proof of Lemma 4. □

Step 2. Using Lemma 4 above and applying the Arason–Elman–Jacob Theorem 3, we get: There exists a valuation w on K such that $|\mathcal{O}^\times_w/(\mathcal{O}_w \cap T)| \leqslant 2$ and $1 + \mathfrak{m}_w \subset T$. Hence letting $\mathcal{O}^\times_w T \subset K^\times$ be the subgroup generated by T and $\mathcal{O}_w$, one has $\mathcal{O}_w/(\mathcal{O}_w \cap T) = (\mathcal{O}^\times_w T)/T$, thus $|(\mathcal{O}^\times_w T)/T| \leqslant 2$. We claim that one actually has $\mathcal{O}^\times_w \subset T$. Indeed, first, one has $k^\times = \mathcal{O}^\times_v \cdot \pi^{\mathbb{Z}}$ as direct sum, hence $(k^\times/p)/(\mathcal{O}^\times_v/p) = \pi^{\mathbb{Z}/p}$. Second, by definitions one has that $K^\times/p = \Sigma/p \cdot k^\times/p$ and $T/p = \Sigma/p \cdot \mathcal{O}^\times_v/p$, both of which being direct sums. Thus finally one gets that

$$K^\times/p = \Sigma/p \cdot k^\times/p = \Sigma/p \cdot \mathcal{O}^\times_v/p \cdot \pi^{\mathbb{Z}/p} = T/p \cdot \pi^{\mathbb{Z}/p}$$

where the dot denotes direct sums, in particular, one has $|K/T| = |(K^\times/p)/(T/p)| = p$. Hence considering the canonical inclusions of groups $T \subseteq \mathcal{O}^\times_w T \subseteq K^\times$, conclude that the order $|(\mathcal{O}^\times_w T)/T| \leqslant 2$ must divide the order $|K^\times/T| = p$. Since $2 < p$, we conclude that $|(\mathcal{O}^\times_w T)/T| = 1$, thus $T = \mathcal{O}^\times_w T$, hence $\mathcal{O}^\times_w \subset T$ is the only possibility. Since $|K^\times/T| = p$, thus $K^\times/\mathcal{O}^\times_w| \geqslant p$, we conclude:

- The valuation w is a *non-trivial* valuation of K.

Step 3. Recalling that $\mathcal{O}_w^\times \subset T$, one has that the canonical projection $K^\times/\mathcal{O}_w^\times \to K^\times/T$ is surjective. Therefore, if $b \in K$ is a generator of $K^\times/T$, e.g., $b = \pi \in k_0$ has $v_0(\pi) = 1$, then b is not a w-unit and $w(b)$ is not divisible by p in $wK = K^\times/\mathcal{O}_w^\times$, hence wK is not divisible by p.

For every subfield $K_\alpha \subset K$ as in the proof of Lemma 4, let $v_\alpha := w|_{K_\alpha}$ be the restriction of w to K_α. Then $\mathcal{O}_{v_\alpha} = \mathcal{O}_w \cap K_\alpha$, and therefore, $\mathcal{O}_{v_\alpha}^\times$ is contained in $T_\alpha = T \cap K_\alpha$.

Lemma 5. *The restriction $v_\alpha := w|_{K_\alpha}$ of w to K_α equals the p-adic valuation w_α.*

Proof. By the first part of the proof of Lemma 4, we have that ${\mathcal{O}^\times}_{w_\alpha} \subset T_\alpha$. Since ${\mathcal{O}^\times}_{v_\alpha} \subseteq T_\alpha$ as well, it follows that the element wise product $\mathcal{O}_{w_\alpha}^\times \mathcal{O}_{v_\alpha}^\times$ is contained in T_α. Since T_α is a proper subgroup of $K_\alpha^\times$ it follows that that $\mathcal{O}_{w_\alpha}^\times \mathcal{O}_{v_\alpha}^\times \neq K^\times$ as well. The following is well known valuation theoretical non-sense: Let $\mathfrak{n}$ be the largest common ideal of $\mathcal{O}_{v_\alpha}$ and $\mathcal{O}_{w_\alpha}$. Then $\mathcal{O} := \mathcal{O}_{v_\alpha}\mathcal{O}_{w_\alpha}$ equals both the localization of $\mathcal{O}_{v_\alpha}$ at $\mathfrak{n}$ and the localization $\mathcal{O}_{w_\alpha}$ at $\mathfrak{n}$. Further, $\mathcal{O}$ is the smallest valuation ring of K which contains both $\mathcal{O}_{v_\alpha}$ and $\mathcal{O}_{w_\alpha}$; or equivalently, $\mathcal{O}$ is the valuation ring of the finest common coarsening of v_α and w_α. We now claim that one has:

$$\mathcal{O}^\times = \mathcal{O}_{v_\alpha}^\times \mathcal{O}_{w_\alpha}^\times.$$

Indeed, let v_α^1 and w_α^1 be the valuations of $\kappa(\mathfrak{n}) := \mathcal{O}/\mathfrak{n}$ defined by $\mathcal{O}_{w_\alpha}/\mathfrak{n}$, respectively $\mathcal{O}_{v_\alpha}/\mathfrak{n}$. Then v_α^1 and w_α^1 are independent, one has exact sequences

$$1 \to (1+\mathfrak{n}) \to {\mathcal{O}^\times}_{v_\alpha} \to \mathcal{O}_{v_\alpha^1}^\times \to 1 \quad \text{and} \quad 1 \to (1+\mathfrak{n}) \to {\mathcal{O}^\times}_{w_\alpha} \to \mathcal{O}_{w_\alpha^1}^\times \to 1.$$

Since v_α^1 and w_α^1 are independent valuations of $\kappa(\mathfrak{n})$, one has that $\mathcal{O}_{v_\alpha^1}^\times \mathcal{O}_{w_\alpha^1}^\times = \kappa(\mathfrak{n})^\times$, and therefore

$$\big(\mathcal{O}_{v_\alpha}^\times \mathcal{O}_{w_\alpha}^\times\big)/(1+\mathfrak{n}) = \kappa(\mathfrak{n})^\times.$$

On the other hand, one also has $\mathcal{O}^\times/(1+\mathfrak{n}) = \kappa(\mathfrak{n})^\times$. Further, $1+\mathfrak{n}$ is contained in both $\mathcal{O}_{v_\alpha}^\times$ and $\mathcal{O}_{w_\alpha}^\times$, hence we conclude that $\mathcal{O}_{v_\alpha}^\times \mathcal{O}_{w_\alpha}^\times = \mathcal{O}^\times$, as claimed.

By contradiction, suppose that $\mathcal{O}_{v_\alpha} \neq \mathcal{O}_{w_\alpha}$. Recall that the valuation ring $\mathcal{O}_{w_\alpha}$ has finite residue field, hence $\mathcal{O}_{w_\alpha}$ is minimal among the valuation rings of K_α, and in particular, $\mathcal{O}_{v_\alpha}$ cannot be contained in $\mathcal{O}_{w_\alpha}$. Therefore, in the above notations, one has that $\mathcal{O}_{w_\alpha} \subset \mathcal{O}$ strictly, or equivalently, $\mathfrak{n} \subset \mathfrak{m}_{w_\alpha}$ is a strict inclusion. On the other hand, if $b \in k$ is any element of minimal positive value 1_v, then $\mathfrak{m}_{w_\alpha} = b\,\mathcal{O}_{w_\alpha}$, and therefore, $b \notin \mathfrak{n}$. Thus we have

$$b \in \mathcal{O}^\times = \mathcal{O}_{v_\alpha}^\times \mathcal{O}_{w_\alpha}^\times \subseteq T_\alpha,$$

contradicting the fact that $w(b)$ generates $wK/w(T) \cong \mathbb{Z}/p$. Thus we conclude that one must have $\mathcal{O}_{w_\alpha} = \mathcal{O}_{v_\alpha}$, and Lemma 5 is proved. $\square$

We next claim that w is a p-adic valuation of K having p-adic rank $d_w = d_v$. Indeed, for $t \in \mathcal{O}_w$, let $K_\alpha \subset K$ be the relative algebraic closure of $k(t)$ in K. Then $K_\alpha|k$ has transcendence degree $\leqslant 1$, and therefore, $w|_{K_\alpha} = w_\alpha$ is the p-adic valuation w_α by Lemma 5. In particular, if $b \in k$ is such that $v(b) = 1_v$ is the minimal positive element of $v(k^\times)$, it follows that $w_\alpha(b)$ is the minimal positive element of $w_\alpha K_\alpha$ under $vk \hookrightarrow w_\alpha K_\alpha$, and further, $kv = K_\alpha w_\alpha$ is the finite field of cardinality $f_v = f_{w_\alpha}$. One has the following:

a) $w(b)$ is the minimal positive element of $w(K^\times)$. Indeed, for $t \in \mathfrak{m}_w$, in the above notations one has: $w(t) = w_\alpha(t) \geqslant w_\alpha(b) = w(b)$.
b) $kv = Kw$ thus $f_v = f_{w_\alpha}$. Indeed, if $t \in \mathcal{O}_w$, then in the above notations, the residue $\bar{t} \in Kw$ satisfies: $\bar{t} \in K_\alpha w_\alpha = kv$.

Therefore, w is a p-adic valuation of rank $d_w = d_v$, which is unique, by the uniqueness of $w_\alpha = w|_{K_\alpha}$ for every subfield K_α. This concludes the proof of Theorem B.

4. Proof of the other announced results

A) *Proof of Theorem A*

The following stronger assertion holds (from which Theorem A immediately follows):

Theorem 6. *Let $k|\mathbb{Q}_p$ be a finite extension containing the p^{th} roots of unity, and let $k_0 \subseteq k$ be a subfield which is relatively algebraically closed in k. Let X_0 be a complete smooth k_0-variety, and $K_0 = k_0(X)$ be the function field of X_0. The following hold:*

1) *Every k-rational point $x \in X_0$ gives rise to a bouquet of conjugacy classes of liftable sections s'_x of $\mathrm{Gal}(K'_0|K_0) \to \mathrm{Gal}(k'_0|k_0)$ above x.*
2) *Suppose that $p > 2$, and let s' be a liftable section of $\mathrm{Gal}(K'_0|K_0) \to \mathrm{Gal}(k'_0|k_0)$. Then there exists a unique k-rational point $x \in X_0$ such that s' equals one of the sections s'_x above.*

Proof. The proof is very similar to the proof of Theorem A of Pop [P2]. We repeat here the arguments briefly for reader's sake.

To 1): Let v be the valuation of k. We notice that by Section 2, C), b), there exists a bijection from the set of (equivalence classes of) p-adic valuations w of $K_0 = \kappa(X_0)$ with $d_w = d_v$ onto the set of bouques of liftable sections above k-rational points x of X_0, which sends each w to the corresponding bouquet of liftable sections above the center x of the canonical coarsening w_1 on $X = X_0 \times_{k_0} k$. Conclude by applying assertion 1) of Theorem B.

To 2): Since $k_0 \subseteq k$ is relatively algebraically closed, it follows that k_0 is p-adically closed. Let v be the valuation of k and of all subfields of k. Since k_0 is p-adically closed, we can apply Theorem B and get: For every liftable section s' of $\mathrm{Gal}(K'_0|K_0) \to \mathrm{Gal}(k'_0|k_0)$, there exists a unique p-adic valuation w of K_0 which prolongs v to K_0 and has p-adic rank equal to the p-adic rank of v, such that s' is a section above w. Let w_1 be the canonical coarsening of w. Then we have:

<u>Case 1</u>. The valuation w_1 is trivial.

Then w is a discrete p-adic valuation of K prolonging v to K, having the same residue field and the same value group as v. Equivalently, the completions of k_0 and K_0 are equal, hence equal to k. Therefore, w is uniquely determined by the embedding $\imath_w : (K_0, w) \hookrightarrow (k, v)$. In geometric terms, $\imath_w$ defines a k-rational point x of X_0, etc.

<u>Case 2</u>. The valuation w_1 is not trivial.

Then w_1 is a k_0-rational place of K_0, hence defines a k_0-rational point x_0 of X_0; hence by base change, a k-rational point x of X_0 as well, etc. □

B) *Proof of Theorem B^0*

The proof is almost identical with the one of Theorem B^0 from Pop [P2]. The proof of assertion 1) is identical with the proof of assertion 1) of Theorem B, thus we omit it. Concerning assertion 2), let $s'_L : \mathrm{Gal}(k'|l) \to \mathrm{Gal}(K'|L)$ be a liftable section of $pr'_L : \mathrm{Gal}(K'|L) \to \mathrm{Gal}(k'|l)$. Then the restriction of s'_L to $\mathrm{Gal}(k'|k) \subseteq \mathrm{Gal}(k'|l)$ gives rise to a liftable section $s' : \mathrm{Gal}(k'|k) \to \mathrm{Gal}(K'|K)$ of $pr'_K : \mathrm{Gal}(K'|K) \to \mathrm{Gal}(k'|k)$. Hence by Theorem B, there exists a unique p-adic valuation w^1 of K which prolongs the p-adic valuation v_k of k to K and has $d_{w^1} = d_{v_k}$, and $s' = s_{w^1}$ in the usual way. Let $w = w^1|_L$ be the restriction of w^1 to L. Then w prolongs the valuation v of l to L. We claim that w^1 is the unique prolongation of w to K. Indeed, let $w^2 := w^1 \circ \sigma_0$ with $\sigma_0 \in \mathrm{Gal}(k|l)$, be a further prolongation of w to K. Then if $(w^i)'$ is a prolongation of w^i to K', $i = 1, 2$, and $\sigma \in \mathrm{im}(s'_L)$ is a preimage of σ_0, then $(w^2)' := (w^1)' \circ \sigma$ is a prolongation of w^2 to K'. Therefore, if $Z_{w^1} \subset \mathrm{Gal}(K'|K)$ is the decomposition group above w^1, then $Z_{w^2} := \sigma Z_{w^1} \sigma^{-1}$ is the decomposition group above w^2. On the other hand, $\mathrm{im}(s') \subseteq Z_{w^1}$ by Theorem B. Since $\sigma \in \mathrm{im}(s'_L)$, and $\mathrm{Gal}(k'|k)$ is a normal subgroup of $\mathrm{Gal}(k'|l)$, thus $\mathrm{im}(s')$ is normal in $\mathrm{im}(s'_L)$, it follows that $\sigma\big(\mathrm{im}(s')\big)\sigma^{-1} = \mathrm{im}(s')$. Hence $\mathrm{im}(s') \subseteq Z_{w^1} \cap Z_{w^2}$. But then by the uniqueness assertion of Theorem B, we must have $w^1 = w^2$. Equivalently, $\mathrm{im}(s'_L)$ is contained in $Z_w \subset \mathrm{Gal}(K'|L)$. Finally conclude that $d_w = d_v$, as claimed, and this concludes the proof of Theorem B^0.

C) *Proof of Theorem* A^0

The following stronger assertion holds (from which Theorem A^0 follows immediately):

Theorem 7. *Let $l|\mathbb{Q}_p$ be a finite extension. Let $l_0 \subset l$ a relatively algebraically closed subfield, and $k_0|l_0$ a finite Galois extension with $\mu_p \subset k_0$. Let Y_0 be a complete smooth geometrically integral variety over l_0. Let $L_0 = \kappa(Y_0)$ the function field of Y_0, and $K_0 = L_0 k_0$.*

1) *Every l-rational point $y \in Y_0$ gives rise to a bouquet of conjugacy classes of liftable sections s'_y of $\mathrm{Gal}(K'_0|L_0) \to \mathrm{Gal}(k'_0|l_0)$ above y.*
2) *Let $p > 2$, and $s' : \mathrm{Gal}(k'_0|l_0) \to \mathrm{Gal}(K'_0|L_0)$ be a liftable section of $\mathrm{Gal}(K'_0|L_0) \to \mathrm{Gal}(k'_0|l_0)$. Then there exists a unique l-rational point $y \in Y_0(l)$ such that s' equals one of the sections s'_y introduced at point* 1) *above.*

Proof. The proof is identical with the proof of Theorem 4.1 above, with the only difference that one uses Theorem B^0, in stead of Theorem B. □

Acknowledgements

I would like to thank among others Jordan Ellenberg, Moshe Jarden, Dan Haran, Minhyong Kim, Jochen Koeningsmann, Jakob Stix, Tamás Szamuely, Adam Topaz, for useful discussions concerning the topic and the techniques of this manuscript.

References

[AEJ] Arason, J., Elman, R. and Jacob, B., *Rigid elements, valuations, and realization of Witt rings,* J. Algebra **110** (1987), 449–467.

[A–K] Ax, J. and Kochen, S., *Diophantine problems over local fields* III. *Decidable fields,* Annals of Math. **83** (1966), 437–456.

[Ef] Efrat, I. *Construction of valuations from K-theory,* Math. Res. Lett. **6** (1999), 335–343.

[Fa] Faltings, G., *Curves and their fundamental groups* (following Grothendieck, Tamagawa and Mochizuki), Astérisque, Vol **252** (1998), Exposé 840.

[GGA] Geometric Galois Actions I, LMS LNS Vol **242**, eds L. Schneps – P. Lochak, Cambridge Univ. Press 1998.

[G1] Grothendieck, A., *Letter to Faltings,* June 1983. See [GGA].

[G2] Grothendieck, A., *Esquisse d'un programme,* 1984. See [GGA].

[Ko1] Koeningsmann, J., *From p-rigid elements to valuations* (*with a Galois-characterization of p-adic fields*)*,* J. Reine Angew. Math. **465** (1995), 165–182. With an *Appendix* by Florian Pop.

[Ko2] Koenigsmann, J., *On the 'section conjecture' in anabelian geometry,* J. reine angew. Math. **588** (2005), 221–235.

[KPR] Kuhlmann, F.-V., Pank, M., Roquette, P., *Immediate and purely wild extensions of valued fields,* Manuscripta Math. **55** (1986), 39–67.

[NSW] Neukirch, J., Alexander Schmidt, Kay Wingberg, *Cohomology of Number Fields,* Grundlehren der mathem. Wissenschaften **323**, 2nd edition., Springer 2000/2008.

[P1] Pop, F., *Galoissche Kennzeichnung p-adisch abgeschlossener Körper*, J. reine angew. Math. **392** (1988), 145–175.

[P2] Pop, F., *On the birational p-adic section conjecture*, Compositio Math. **146** (2010), 621–637.

[P–R] Prestel, A. and Roquette, P., Formally p-adic fields, LNM 1050, Springer Verlag 1985.

[St] Stix, J., *Birational p-adic Galois sections in higher dimensions,* Israel Journal of Mathematics **198** (2013), 49–61.

[Sz] Szamuely, T., *Groupes de Galois de corps de type fini,* (d'après Pop), Astérisque, Vol. **294** (2004), 403–431.

[To] Topaz, A., *Commuting-Liftable Subgroups of Galois Groups II,* J. reine angew. Math. (to appear). See `arXiv:1208.0583 [math.NT]`.

[Wa] Ware, R. *Valuation rings and rigid elements in fields,* Canadian J. Math. **33** (1981), 1338–1355.

Florian Pop pop@math.upenn.edu
Department of Mathematics
University of Pennsylvania
DRL, 209 S 33rd Street
Philadelphia, PA 19104. USA

http://math.penn.edu/~pop